Cyberattacks: Threatening the Value of Your Technology Company
Cybersecurity, at its core, is about protecting what’s valuable to you as a company.

For some, that might mean protecting valuable customer data—credit card information, Social Security numbers, or patient health care records. For technology companies, it’s also about protecting intellectual property. This includes source code, designs, products, or future product strategies. Collectively, that intellectual property defines the value of a tech company, and that value is usually sitting on a server as an easy target to be hacked.

Indeed, for many organizations, it’s no longer a question of whether a network will be compromised but when a network will be compromised. Almost 50 percent of all companies experienced at least one security incident during a 12-month period, according to a 2016 survey by the Ponemon Institute. If that isn’t an impressive enough figure, then consider this: The average data breach costs a company $6.5 million.

That’s a frightening perspective with a huge cost attached to it—and things aren’t going to get better anytime soon.

The rapid proliferation of new technology, including a wide array of mobile devices and cloud-based solutions, means that hackers now have many more entry points to attack. Additional vigilance is required for larger companies because of their access to valuable information and pervasive technologies, which makes them a natural target. This doesn’t let the small guy off the hook, though. If there are rumblings that a start-up has the next killer app in development, for example, they’re vulnerable to attack.

Economic espionage, or cyberespionage, isn’t limited to borders. It isn’t uncommon for overseas companies to target entities releasing products with high potential for profit and revenue. While the act itself isn’t necessarily something new, there are now organized and contracted teams leading the attack.

Even with stronger security defenses, organizations are still at a disadvantage in the fight against hackers. Why? Because cyberattacks are increasingly aimed at individuals rather than systems—and the human factor is much harder to manage. People, however, are also the first line of defense with proper training.
It’s no longer a question of whether a network will be compromised, but when a network will be compromised.

- **50%**
  Companies that experienced at least one security incident
  Source: Ponemon Institute

- **500+ billion**
  Total number of personal records stolen or lost.

- **$6.5 million**
  Average cost a company pays for a data breach.
  Source: Ponemon Institute

- **$445 billion**
  Total cost of data breaches and cybercrime worldwide.
  Source: 2014 joint study by antivirus software maker McAfee and the Center for Strategic and International Studies
Attack Targets

Attackers are increasingly sophisticated and have more access points to networks, including mobile phone devices. It’s important to remember that professionals typically hack people, they don’t go after the system.

Common Cyberattack Approaches

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPEAR PHISHING</td>
<td>This is an e-mail that asks for information—IT system access data or bank details—in the hopes of someone innocently responding and providing it.</td>
</tr>
<tr>
<td>WHALING</td>
<td>This method is the same as spear phishing but targets C-level executives.</td>
</tr>
<tr>
<td>RANSOMWARE</td>
<td>Hackers gain access to a system using malicious software, then encrypt sensitive data and hold it hostage—along with your ability to conduct business—until a demand is satisfied.</td>
</tr>
<tr>
<td>INTERNET OF THINGS</td>
<td>This includes many different types of devices that perform a single function at low processing power and lack security functions.</td>
</tr>
</tbody>
</table>

Source: Symantec’s Internet Security Threat Report 2016
Phishing

**SPEAR PHISHING**
Sophisticated attacks usually begin here. A social engineering attack preys on the psychological willingness of employees to divulge a company's confidential digital information. These attacks involve an e-mail from a hacker who appears to be an individual or business you know. The target tends to be an unaware or untrained employee who may be willing to give up desirable information—their system password or company account details, for example.

**WHALING**
When the target is C-level executives, it's known as whaling. C-level e-mail fraud takes place when a hacker requests that members of an organization's finance function disburse or wire funds to a third-party in an e-mail that looks like it comes from senior management. (See example at right.)

**DEFENSE STRATEGY**
It's important to remember there isn't an all-encompassing solution to combat spear phishing or whaling. Prior to an attack, these defenses should be in place:

- **End-User Security Training**
  Never forget that people are your first line of defense.

- **Technical Controls**
  This includes e-mail system security, including antispam, URL scanning, and attachment stripping.

- **Internal Process Controls**
  Have at least two sets of eyes and approval for requests that meet a certain threshold.

**WHALING EXAMPLE**

Hi Joe
Mary CEO
February 29, 2016 at 10:44 AM
To: Joe.CFO@example.com

Hi Joe
Are you in the office? Kindly let me know because I need you to send out an important payment for me today.

Thank you,
Mary CEO
Sent from my iPhone

In this example, someone named Mary is e-mailing Joe, the CFO of a company, to urgently request payment. What should Joe do?

Joe's first step should be to slow down and think about the validity of a request when it comes in. He should take the time to hover over any hyperlinks to see where it's going or check the e-mail address carefully to be sure it isn't a fabricated account.
Ransomware

Also known as scareware, this software allows hackers to access an employee’s computer, encrypt sensitive data, and then demand some form of payment to decrypt it. Often beginning with a spear-phishing attack, it infects the system and can propagate from there. McAfee Labs researchers saw more than 4 million instances of ransomware in the second quarter of 2015 alone and expect this number to continue growing.

DEFENSE STRATEGY

There are administrative and technical controls to employ in this situation.

**Administrative Controls**
- End-user security awareness training
- Internal process controls
- Disaster recovery and business continuity plans
- Contact information for local law enforcement, the FBI, and service providers

**Technical Controls**
- Frequent backups and snapshots of databases
- Test backups for key systems
- Network segmentation
- Up-to-date antivirus and system software through frequent patching
- Near real-time monitoring services, such as firewall information networks
The Going Price of Data

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>$3–$5</td>
</tr>
<tr>
<td>Including name</td>
<td></td>
</tr>
<tr>
<td>Credit Card (Basic Info)</td>
<td>$2–$4</td>
</tr>
<tr>
<td>Including number, type, expiration date, CVV number, and account holder's name</td>
<td></td>
</tr>
<tr>
<td>Credit Card (Premium Info)</td>
<td>$35–$40</td>
</tr>
<tr>
<td>Including basic credit card info, account holder's SSN, address, and DOB</td>
<td></td>
</tr>
<tr>
<td>PayPal Account</td>
<td>$20–$35</td>
</tr>
<tr>
<td>Medical Record</td>
<td>$50</td>
</tr>
<tr>
<td>Including SSN, banking details, demographic, job details</td>
<td></td>
</tr>
</tbody>
</table>

Source: 2015 study by Trend Micro

While these figures are good reference points, it's important to note that the price of data fluctuates frequently according to the market.
Internet of Things

Another entry point for hackers is the Internet of Things, or IoT. These devices—a wireless HVAC controller, smart watch, or even a drug-infusion pump that dispenses medication based on a patient’s physiological alerts—are particularly vulnerable because vendors are rushing to push products to market without considering the design of security elements.

Security and privacy are also hindered by the fact that a myriad of manufacturers have too many different types of devices, which typically have low processing power, are designed to perform a single function, and aren’t secured with universally accepted security standards.

**OTHER EXAMPLES OF IOT DEVICES:**
- AVL sensor in a public transportation card
- Smart video conferencing systems
- Radio frequency identification (RFID) systems used for inventory
- Vending machines
- Fitbits

**DEFENSE STRATEGY**
- Know where IoT devices are in the environment
- Develop a policy for governing the use of IoT devices in the environment
- Have governance and risk assessment processes in place when new IoT devices are considered
- Use a separate wireless network to separate devices from the corporate network
- Use encryption while data is in transit, especially for sensitive information, if possible

90% of consumer products will have the ability to interact with other devices in 2015.

Source: Samsung

26–50 billion IoT devices will be connected by 2020.

Sources: Gartner and Cisco, respectively
Accountability

High-profile enterprise hacking leads to the painful loss of precious data, customer confidence, and hundreds of millions of dollars in legal fees, notification costs, and technology remediation.

It’s no wonder C-level executives are now paying more attention to their organizations’ vulnerabilities when it comes to cybersecurity. Other individuals also demand results:

- **Investors and boards of directors** are increasingly holding senior management accountable for cybersecurity.

- **Customers and partners** demand adequate cybersecurity controls are in place before conducting business.

- **US states, regulators, and regulatory bodies** are legally mandating cybersecurity compliance.

**STANDARDS AND GUIDELINES**

Companies are also embracing new cybersecurity standards and guidelines.

- **National Institute of Standards and Technology’s Cybersecurity Framework (NIST CSF)**

- **Special Publication 800-53, Revision 4 (NIST SP 800-53r4)**

- **International Standards Organization (ISO) 27001**
Cost of Each Record Hacked
by industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>$398</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>$298</td>
</tr>
<tr>
<td>Financial</td>
<td>$259</td>
</tr>
<tr>
<td>Energy</td>
<td>$256</td>
</tr>
<tr>
<td>Transportation</td>
<td>$252</td>
</tr>
<tr>
<td>Communications</td>
<td>$237</td>
</tr>
<tr>
<td>Education</td>
<td>$225</td>
</tr>
<tr>
<td>Services</td>
<td>$219</td>
</tr>
<tr>
<td>Consumer</td>
<td>$218</td>
</tr>
<tr>
<td>Industrial</td>
<td>$190</td>
</tr>
<tr>
<td>Retail</td>
<td>$189</td>
</tr>
<tr>
<td>Media</td>
<td>$185</td>
</tr>
<tr>
<td>Technology</td>
<td>$178</td>
</tr>
<tr>
<td>Research</td>
<td>$166</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$135</td>
</tr>
<tr>
<td>Public</td>
<td>$73</td>
</tr>
<tr>
<td><strong>AVERAGE</strong></td>
<td>$217</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute
Common Cybersecurity Issues for Organizations

A cybersecurity attack is often adapted for a particular company or industry. Here are five common problems that make organizations especially vulnerable to cyberattacks.

01  
*Excessive Administrator-Level Access* to networks and systems

We’ve seen instances where vendors, consultants, and outside contractors retain access long after engagements with organizations are completed.

02  
*Excessive Physical Access* to data centers and server rooms

In many cases, this broad-based access doesn’t have a business need and often leads to data breaches.

03  
*Inadequate Cybersecurity Awareness* among executives and employees

Training is essential so that staff at all levels are aware of cybersecurity risks and how to recognize and avoid them. This training should be included in a mandatory HR best practices portfolio and conducted annually.

04  
*Inadequate Disaster Recovery Plan*

A proper plan should include steps to deal with destructive data loss or a security breach. A number of companies are ill-prepared to cope with this type of crisis, and the ensuing damage and recovery time can be exponential.

05  
*Prioritizing Convenience*

Too many organizations, especially smaller ones, choose convenience over high-level cybersecurity. For example, they have one flat network that doesn’t contribute to a layered defense rather than a segmented structure. This prevents a company from containing a security breach in one isolated part of the network.
RECENT CYBERATTACKS

DECEMBER 2013
Target had 70 million customer identities stolen.

JULY–AUGUST 2014
JPMorgan Chase discovered unauthorized individuals accessed more than 90 of its secure servers over a two-month period. The result was the loss of personal financial information for at least 76 million households.

NOVEMBER 2014
Sony Pictures found that e-mail systems were accessed and embarrassing discussions were made public with costly consequences.

JANUARY 2015
Anthem Blue Cross Insurance Companies, the nation’s second largest insurer, disclosed a breach in which the identities of 80 million customers were potentially stolen.

FEBRUARY 2015
Intuit had to warn its TurboTax customers to hold off from filing tax returns to ensure hackers couldn’t steal their refunds.

FEBRUARY 2016
Hollywood Presbyterian Medical Center paid a hacker $17,000 in bitcoin after a ransomware attack encrypted its electronic medical record system, effectively locking the hospital out of its records for a week.
Assessing Your Vulnerabilities

IT Security Risk Assessment and Analysis

There are many ways to infiltrate a company. Often, a company’s biggest weakness is not knowing how exposed it is to a cyberattack. An IT security risk assessment and analysis can help identify and assess the holes in your operation—a good first step toward protecting your organization.

A risk assessment can help answer several key questions:

- What systems are most at risk?
- Who has access to the most significant organizational data?
- How was mission-critical data acquired?
- What vital data is being processed, and how?
- What essential data is being stored, and how?
- What valuable data is being transmitted, and how?
- Where is crucial data being transmitted?

A cybersecurity risk assessment and analysis needs to be conducted annually and should focus on internal cybersecurity controls each year as well. It’s important to know what cybersecurity controls are installed as well as if those controls are working and up to date.

Examine these cybersecurity controls on a regular basis:

- **Administrative Security Controls**
  Policies and procedures related to IT security, incident response plans, and disaster recovery plans

- **Technology Controls**
  Networks, servers, mobile devices, and workstations

- **Physical Controls**
  Access rights to your data center and server rooms

- **Operational Controls**
  Approval processes

- **Social Engineering Controls**
  Confront the newest forms of people-driven cyberattacks through security awareness training

Penetration Testing

In addition to conducting a cybersecurity risk assessment and analysis and focusing on internal cybersecurity controls, prudent cybersecurity management also requires penetration testing.

Penetration testing allows highly skilled and experienced security consultants to identify vulnerabilities by invading your systems from a cyberattacker’s perspective. Put another way, penetration testing is “ethical” hacking.

Among other things, penetration testing helps identify:

- Holes and flaws in IT systems
- Patches that were installed to fix issues
- Incorrect or inadequate configurations
- Updates and upgrades that have and haven’t been performed
Due Diligence with Third-Party Hosting Services

If you use cloud-based or third-party hosting services or other services that help manage an aspect of your technology environment, such as firewall management or data backup, then you should ascertain the protections and security measures the vendor has in place to protect client data.

Audits: Attestation Reports on Controls

A company should request and review a Service Organization Control (SOC) examination report, also known as SSAE 16. Alternatively, utilize an ISO 27001 audit by an independent and objective firm that specializes in technology audits before entering into an agreement with the service provider and giving them access to your sensitive data.

In addition, the contract between your organization and the service provider should include language that allows you to conduct audits of their hosting environment.

WE’RE HERE TO HELP

Cybersecurity is a bit like playing cat and mouse. The risk of a breach will always be present, but staying one step ahead and being aware of evolving cybersecurity threats will go a long way toward enhancing your organization’s security.

If you’d like to learn more, contact your Moss Adams professional or visit www.mossadams.com/technology. You can also subscribe to have relevant articles, news, and event notifications sent to you via e-mail.
In the Unfortunate Event of a Breach

If your organization does experience a data breach, there are immediate steps that should be taken to stem the damage and minimize the impact as well as to stay compliant with regulatory requirements.

01 **Exercise Your Security Incident Response Plan**

When a breach occurs, time is of the essence. Having an incident response plan is instrumental in alleviating the pressure of making decisions.

02 **Bring In a Fresh Set of Eyes**

This perspective often comes from a third-party that specializes in computer forensics or postattack analysis; the FBI has a division that investigates cybersecurity breaches, for example. The objective is to reveal clues or leads and offer external assistance when IT staff, who are often too close to the situation, might get weary-eyed and lose focus.

03 **Know Your Notification Responsibilities**

Federal and state-specific regulations mandate that affected parties be notified of any data breach that involves their personal information. It’s important to know what your organization’s obligations are from a compliance standpoint to avoid potential monetary penalties, fines, and lawsuits.

A typical plan should include:

- Roles and responsibilities
- Trigger incidents
- Technology environment overview, including a network diagram, containment procedures, and eradication and cleanup procedures
- Communications protocols
- A call list, including key vendors the organization is dependent on for technology support
Contact your insurance agent immediately upon stabilizing the situation. Determine what’s covered, which may include fees related to legal, public relations, communications, notifications to external parties, forensics activities, and the overall response effort. Also, determine if theft of proprietary information is covered, particularly if you have intellectual property.

After the situation has stabilized, many organizations fail to learn from their mistakes and don’t implement the controls or protections necessary to prevent a future attack or at least minimize the risk of a successful attack. Developing a remediation plan to address the risk and implement stronger controls and protections is essential to ensuring a similar attack doesn’t occur in the future.

Practice securing data throughout its life cycle. This means considering protections and security controls that should be in place once the data is acquired, when it goes through processing, where it gets stored, and when it’s transmitted or moved.
About Our Technology Practice

Helping technology companies succeed requires deep industry experience and a strong commitment to providing timely, value-added services that go beyond the basics. That's exactly what we bring to our technology clients and their management teams through proactive communication. Our goal for you is to improve operations, prepare for the future, and capitalize on opportunities.

WHO WE SERVE

We serve emerging, institutionally backed start-ups, multinational public enterprises, and everything in between. Our clients work in these areas:

- SaaS
- Hardware and devices
- Digital media
- Gaming and entertainment
- Semiconductors
- Medical devices
- Internet services
- Communications and mobile devices
- Mobile advertising
- Financial technology companies

CYBERSECURITY SERVICES

- IT security assessments
- Network vulnerability assessments and penetration testing
- Web application penetration testing
- Security analytics
- Wireless network assessments
- Social engineering
- Disaster recovery and business continuity planning
- Application code security reviews

PROFESSIONAL AFFILIATIONS

Our professionals are members of a number of information security associations, including:

- Information Systems Audit and Control Association
- Information Systems Security Association
- International Information Systems Security Certification Consortium
- Institute of Internal Auditors
- Cloud Security Alliance

CONTACTS

Kevin Villanueva  
Director, IT Auditing & Consulting Practice  
(206) 302-6542  
kevin.villanueva@mossadams.com

Taft Kortus  
Industry Group Leader, Technology, Communications & Media  
(206) 302-6377  
taft.kortus@mossadams.com

Francis Tam  
Partner, IT Auditing & Consulting Practice  
(310) 295-3852  
francis.tam@mossadams.com

MOSS ADAMS LLP  
Certified Public Accountants | Business Consultants
Learn more at
www.mossadams.com/technology.
ABOUT MOSS ADAMS

Nationwide, Moss Adams and its affiliates provide insight and expertise integral to your success.

**Moss Adams LLP** is a national leader in assurance, tax, consulting, risk management, transaction, and private client services.

**WWW.MOSSADAMS.COM**

**Moss Adams Wealth Advisors LLC** provides investment management, personal financial planning, and insurance strategies to help you build and preserve your wealth.

**WWW.MOSSADAMSWEALTHADVISORS.COM**

**Moss Adams Capital LLC** offers investment banking and strategic advisory services, helping you create greater value in your business.

**WWW.MOSSADAMSCAPITAL.COM**